

REMARKS

The application has been reviewed in light of the Office Action dated November 10, 2004. Claims 1-20 are pending in this application, with claims 1, 10-12 and 14 being in independent form. By the present Amendment, claim 9 has been amended to correct formal matters. It is submitted that no new matter has been added and no new issues have been raised by the present Amendment.

Claim 9 was objected to because of an informality. In response, claim 9 has been amended with particular attention to the points raised in the Office Action. Withdrawal of the objection to claim 9 is respectfully requested.

Claims 1-7 and 10-19 were rejected under 35 U.S.C. §102(b), as allegedly anticipated by U.S. Patent No. 5,398,196 to Chambers. Claims 8, 9 and 20 were rejected under 35 U.S.C. §103(a) as allegedly obvious from Chambers and further in view of U.S. Patent 5,974,549 to Golan. Applicants have carefully considered the Examiner's comments and the cited art, and respectfully submit independent claims 1, 10-12 and 14 are patentably distinct from the cited art, for at least the following reasons.

Independent claim 1 relates to a method of detecting viral code in subject files, comprising, creating an artificial memory region spanning one or more components of the operating system, emulating execution of computer executable code in a subject file, and detecting when the emulated computer executable code attempts to access the artificial memory region.

According to an embodiment of the present disclosure, by using calls to an operating system, the method and apparatus of the subject application are able to detect viral code that may be present in a computer executable file. Of course, the claims are not limited to the disclosed embodiments.

Chambers, as understood by the Applicants, relates to a method and apparatus for detecting computer viruses by emulating the execution of a target program and analyzing the emulated execution to detect viral behavior. For example, a monitor program determines if the target program is attempting to access memory selected for controlled access and if so, the monitor program remaps the memory address so that the original memory location is protected from the target program (Chambers, column 8, lines 4-14). In other words, as understood by the Applicants, while emulating each instruction, the monitor program in Chambers simply blocks instructions that attempt to access memory locations that are selected for controlled access.

However, Chambers is not understood to teach or suggest a method of detecting viral code in subject files, comprising, creating an artificial memory region spanning one or more components of the operating system, emulating execution of computer executable code in a subject file, and detecting when the emulated computer executable code attempts to access the artificial memory region, as recited in independent claim 1.

Accordingly, Applicants submit that independent claim 1 is patentably distinct from the cited art. Independent claims 10-12 and 14 are believed to be patentably distinct for at least similar reasons.

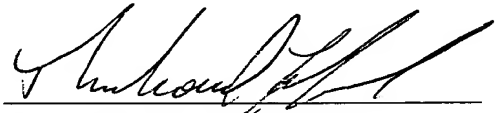
The Office is hereby authorized to charge any additional fees that may be required in connection with this amendment and to credit any overpayment to our Deposit Account No. 03-3125.

If a petition for an extension of time is required to make this response timely, this paper should be considered to be such a petition, and the Commissioner is authorized to charge the requisite fees to our Deposit Account No. 03-3125.

If a telephone interview could advance the prosecution of this application, the Examiner is respectfully requested to call the undersigned attorney.

Entry of this amendment and allowance of this application are respectfully requested.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Richard F. Jaworski', written over a horizontal line.

RICHARD F. JAWORSKI

Reg. No.33,515

Attorney for Applicants

Cooper & Dunham LLP

Tel.: (212) 278-0400